System and Method for Conducting A Secure Response Communication Session

(A-70560/RMA)

WE CLAIM:

1. A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for conducting a secure response session, the program module including instructions for:

A. extracting, by a Client who is establishing a secure response session to a Entity in order to respond to a message from the Entity, the Entity's public key and matching destination address of the Entity from a trusted source or storage means;

B. extracting, by the Client, the Client's public and private key and certificate chain from a trusted source or storage means;

C. using the extracted client public and private key and certificate chain information along with the previously extracted Entity destination address to create a secure session with the Entity using a secure session protocol;

D. sending, by the Client, a first Data message after any session setup messages, that contains a Resource Tag that was included in the message received from the Entity to which this client initiated session is a response;

E. setting up, by the Entity, the session setup portion of the secure session protocol; and

F. verifying, by the Entity, the Client's certificate chain and the Resource Tag that is received in the first Data message from the Client.

2. A hardware architecture neutral and operating system neutral and network transport neutral method for secure response session using less software code and network bandwidth than conventional systems, said method comprising the steps of:

A. extracting, by a Client who is establishing a secure response session to a Entity in order to respond to a message from the Entity, the Entity's public key and matching destination address of the Entity from a trusted source or storage means;

B. extracting, by the Client, the Client's public and private key and certificate chain from a trusted source or storage means;

C. using the extracted client public and private key and certificate chain information along with the previously extracted Entity destination address to create a secure session with the Entity using a secure session protocol;

D. sending, by the Client, a first Data message after any session setup messages, that contains a Resource Tag that was included in the message received from the Entity to which this client initiated session is a response;

E. setting up, by the Entity, the session setup portion of the secure session protocol; and

F. verifying, by the Entity, the Client's certificate chain and the Resource Tag that is received in the first Data message from the Client.

3. The method in Claim 2, further comprising:

G. exchanging, between the Client and the Entity, additional data related to the application that is using the secure response protocol;

4. The method in Claim 2, further comprising:

H. terminating the session, by either the Client or the Entity, by closing the underlying network connection.

5. The method in Claim 4, wherein the underlying network connection is a TCP-based network connection.

6. The method in Claim 4, wherein the public key and matching destination address has been verified previously using a digital signature (verified with a trusted public key) or cryptographic checksum (verified with a trusted key derived from a Master Key or Session Key or Message Key).

7. The method in Claim 2, wherein the Entity's public key comprises a RSA or a RSA based public key.

8. The method in Claim 2, wherein the matching destination address comprises a URL or URL based address.

9. The method in Claim 2, wherein the trusted source or storage means comprises data selected from the set consisting of a normal conventional e-mail message, a non-secured web page, a secured web page, and combinations thereof.

10. The method in Claim 2, wherein the secured web page is secured by any of SSL, PCT, or TLS.

11. The method in Claim 2, wherein the trusted storage means comprises data received from communicating with a Server via a secure session.

12. The method in Claim 2, wherein the Client's keys and certificate chain comprise fixed values.

13. The method in Claim 2, wherein the Client's keys and certificate chain comprise fixed values shared by more than one Client system and wherein the Entity authenticates the Client based on this Resource Tag.

14. The method in Claim 2, wherein the Client's keys and certificate chain are unique to this Client, and the Entity authenticates the Client using this unique certificate and/or using a Resource Tag was included in the message received from the Entity to which this session is a response.

15. The method in claim 2, wherein said Entity comprises a Merchant.

16. A method for conducting a secure response session from a Client that is establishing a secure response session to an Entity in order to respond to a message from the Entity, said method comprising the steps of:

extracting, by the Client, information including the Entity's public key and destination address and Client's public and private key and certificate chain from one or more trusted source;

using, by the Client, the extracted information to create a secure session with the Entity using a secure session protocol; and

sending, by the Client, a first data message that contains a resource tag that was included in the message received from the Entity to which this Client initiated session is a response.

17. The method in claim 16, wherein the first data message is sent after one or more session setup message.

18. The method in claim 16, further comprising:

setting up, by the Entity, the session setup portion of the secure session protocol; and

verifying, by the Entity, the Client's certificate chain and the Resource Tag that is received in the first Data message from the Client.

19. The method in claim 16, wherein said Entity comprises a Merchant.

20. The method in claim 18, wherein said Entity comprises a Merchant.

21. The method of claim 2, wherein the trusted source or storage means comprises a Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root public key.

22. A computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the

computer system and/or components thereof, to function in a specified manner to conduct a secure response session from a Client that is establishing a secure response session to an Entity in order to respond to a message from the Entity and occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for conducting a secure response session, the program module including instructions for:

extracting, by the Client, information including the Entity's public key and destination address and Client's public and private key and certificate chain from one or more trusted source;

using, by the Client, the extracted information to create a secure session with the Entity using a secure session protocol; and

sending, by the Client, a first data message that contains a resource tag that was included in the message received from the Entity to which this Client initiated session is a response.